Nonce IV: Here we think of CBC Mode as a nonce-based encryption scheme, as in Section 11.6.4. We start with the negative result

Theorem 13.5. *With a nonce as the IV, CBC Mode* is not IND-CPA *secure.*

PROOF. Let $\mathbf{0}$ be the all-zero block and $\mathbf{1}$ be the all-one block. The attack on the IND-CPA security is as follows:

- Send the message $\mathbf{0}$ with the nonce $IV = \mathbf{0}$ to the encryption oracle $\mathcal{O}_{e_k}$. The adversary obtains the ciphertext $\mathbf{0}\|c$ in return, where $c = e_k(\mathbf{0})$.
- Now send the messages $m_0 = \mathbf{0}$ and $m_1 = \mathbf{1}$ to the $\mathcal{O}_{\mathsf{LR}}$ oracle, with nonce $\mathbf{1}$. Notice this is a new nonce and so the encryption is allowed in the game. Let $\mathbf{1}\|c^*$ be the returned ciphertext.
- If $c^* = c$ then return $b' = 1$, else return $b' = 0$.

To see why this attack works, note that if the hidden bit is $b = 1$ then the challenger returns c^* which is the evaluation of the block cipher on the block $\mathbf{1} \oplus \mathbf{1} = \mathbf{0}$. Whereas if $b = 0$ then the evaluation is on the block $\mathbf{0} \oplus \mathbf{1} = \mathbf{1}$. □

On the positive side, when used only once nonce-based encryption is identical to a fixed IV, and so CBC Mode used in a nonce-based encryption methodology is IND-PASS secure.

Random IV: With a random IV we can be more positive, since CBC Mode is IND-CPA secure as we will now show.

Theorem 13.6. *With a random IV, CBC Mode is* IND-CPA *secure assuming the underlying block cipher e_k acts like a pseudo-random permutation. In particular let A denote an adversary against CBC Mode which makes q_e queries to its encryption oracle, and let all plaintext submitted to both the* LR *and encryption oracles be at most ℓ blocks in length. Then there is an adversary B such that*

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{CBC}[e_k]}(A; q_e) \leq 2 \cdot \mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + \frac{T^2}{2^{n-1}},$$

where n is the block size of the cipher e_k and $T = (q_e + 1) \cdot \ell$.

PROOF. In the security game the challenger needs to call the underlying block cipher on behalf of the adversary. The total number of such calls is bounded by $T = (q_e + 1) \cdot \ell$.

Our first step in the proof is to replace the underlying block cipher e_k by a pseudo-random permutation. This can be done by the assumption that e_k is a secure PRP, namely there is some adversary B such that

$$\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) = \Big|\Pr[A \text{ wins } \mathsf{CBC}[e_k]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]]\Big| \tag{19}$$

where we let $\mathcal{P}$ denote a random permutation. Our next step is to switch from the component being a random *permutation* to a random *function*. This follows in the same way as we proved the PRF-PRP Switching Lemma (Lemma 11.2). Suppose we replace $\mathcal{P}$ by a random function $\mathcal{F}$ in the CBC game and we let E denote the event, during the game $\mathsf{CBC}[\mathcal{F}]$, that the adversary makes two

calls to $\mathcal{F}$ which result in the same output value. We have

$$\begin{aligned}\Big|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]]\Big| &= \Big|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] \\ &\qquad - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \wedge \neg E] \\ &\qquad - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \wedge E]\Big| \\ &= \Big|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] \\ &\qquad - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \mid E] \cdot \Pr[E]\Big| \\ &\leq \Pr[E] \leq \frac{T^2}{2^{n+1}}, \end{aligned} \tag{20}$$

since if E does not happen the two games are identical from the point of view of the adversary, and by the birthday bound $\Pr[E] \leq \frac{T^2}{2^{n+1}}$.

Our final task is to bound the probability of A winning the CBC game when the underlying "block cipher" is a random function. First let us consider how the challenger works in the game $\mathsf{CBC}[\mathcal{F}]$. When the adversary makes an $\mathcal{O}_{\mathsf{LR}}$ or $\mathcal{O}_{e_k}$ call, the challenger answers the query by calling the random function. As we are dealing with a random function, and not a random permutation, the challenger can select the output value of $\mathcal{F}$ *independently* from the codomain; i.e. it does not need to adjust the output values depending on the previous values. This last point will make our analysis simpler, and is why we switched to the PRF game from the PRP game.

Now notice that the adversary does not control the inputs to the random function at any stage in the game, so the only way he can find any information is by creating an input collision, i.e. two calls the challenger makes to the random function are on the same input values[3].

We thus let M_j denote the event that the adversary makes an input collision happen within the first j calls, and note that if M_T does not happen then the adversary's probability of winning is $1/2$, i.e. the best he can do is guess. We have

$$\begin{aligned}\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]] &= \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \mid M_T] \cdot \Pr[M_T] \\ &\qquad + \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \mid \neg M_T] \cdot \Pr[\neg M_T] \\ &\leq \Pr[M_T] + \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}] \mid \neg M_T] \\ &\leq \Pr[M_T] + \frac{1}{2} \end{aligned} \tag{21}$$

So we are left with estimating $\Pr[M_T]$. After q_e queries to the encryption oracle the adversary has made $T = \ell \cdot (q_e + 1)$ indirect queries to the PRF; since each queries is of length ℓ and we need to also include the challenge ciphertext. Thus the probability of a collision in the inputs to the PRF after T queries is

$$\Pr[M_T] \approx T^2/2^{n+1}.$$

[3]This is why CBC Mode is not secure in the nonce-based setting as in this setting the adversary controls the first input block, by selecting the first block of the message and the IV.

Summing up we have

$$\begin{aligned}
\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{CBC}[e_k]}(A;q_e) &= 2\cdot\left|\Pr[A \text{ wins } \mathsf{CBC}[e_k]] - \frac{1}{2}\right| \\
&= 2\cdot\Big|\Pr[A \text{ wins } \mathsf{CBC}[e_k]] - \frac{1}{2} \\
&\qquad + (\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]])\Big| && \text{adding in zero} \\
&\le 2\cdot\Big|\Pr[A \text{ wins } \mathsf{CBC}[e_k]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]]\Big| \\
&\qquad + 2\cdot\left|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \frac{1}{2}\right| && \text{triangle inequality} \\
&= 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + 2\cdot\left|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \frac{1}{2}\right| && \text{by equation (19)} \\
&= 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + 2\cdot\Big|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \frac{1}{2} \\
&\qquad + (\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]])\Big| && \text{adding in zero} \\
&\le 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) \\
&\qquad + 2\cdot\Big|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{P}]] - \Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]]\Big| \\
&\qquad + 2\cdot\left|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]] - \frac{1}{2}\right| && \text{triangle inequality} \\
&\le 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + \frac{T^2}{2^n} + 2\cdot\left|\Pr[A \text{ wins } \mathsf{CBC}[\mathcal{F}]] - \frac{1}{2}\right| && \text{by equation (20)} \\
&\le 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + \frac{T^2}{2^n} + 2\cdot\Pr[M_T] && \text{by equation (21)} \\
&\le 2\cdot\mathrm{Adv}^{\mathsf{PRP}}_{e_k}(B) + \frac{T^2}{2^{n-1}}.
\end{aligned}$$

□

Let us examine what this means when we use the AES block cipher in CBC Mode. First the block length of AES is $n = 128$, and let us assume the key size is 128 as well. If we assume AES behaves as a PRP, then we expect that

$$\mathrm{Adv}^{\mathsf{PRP}}_{AES}(B) \approx \frac{1}{2^{128}}$$

for all adversaries B. We can now work out the advantage *for any* adversary A to break AES when used in CBC mode, in the sense of IND-CPA. We find

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{CBC}[AES]}(A;q_e) \le \frac{2 + 2\cdot T^2}{2^{128}}.$$

Thus even if the adversary makes 2^{30} calls to the underlying block cipher, the advantage will still be less than

$$\frac{2 + 2\cdot 2^{60}}{2^{128}} \approx 2^{-67},$$

which is incredibly small. Thus as long as we restrict the usage of AES in CBC Mode with a random IV to encrypting around 2^{30} blocks per key we will have a secure cipher. Restricting the usage of a symmetric cipher per key is enabled by requiring a user to generate a new key every so often.